REMARKS

In this Amendment, Applicant has cancelled Claim 2 without prejudice or disclaimer, amended Claims 1 and 3, and added new Claim 5. Claims 1 and 3 have been amended to specify further embodiments of the present invention and overcome the prior art. It is respectfully submitted that no new matter has been introduced by the amended and new claims. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the preceding amendments and the following comments.

REJECTIONS UNDER 35 U.S.C. § 102:

Claims 1 – 3 have been rejected under 35 U.S.C. § 102 (b) as allegedly being anticipated by Schneier (Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons).

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference. More specifically, Claim 2 has been cancelled. The rejection to this claim is moot. In addition, the embodiment of the present invention as defined in the amended Claims 1 and 3 include the feature of "prior to carrying out said two-place operation on an i-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey **depending on the value of a j-th data subblock**, where $i \neq j$" (emphasis added). Such feature is not disclosed or taught by Schneier.

In the Advisory Action, the Examiner indicated that the shift in Schneier is performed before the shifted key is combined with the broadened subblock from the previous permutation to create the current subblock. Applicant respectfully submits that the Examiner's interpretation of Schneier is incorrect, because "[T]he shift is effected before the shifted bit combines with the widened subblock from the previous permutation to create the current block" does not mean that key bit shift is effected by depending on

the value of the subblock of the data being converted or simply data. In Schneier, data supplied to the input change and the key bit shift is always fixed for each round of conversion. If the shift depended on data or a data subblock, the subkey would change at least in one round of encryption depending on the data being converted (input data).

In addition, the Examiner indicated that the previously presented claims do not have the feature argued by the Applicant. It is respectfully submitted that the amended claims clearly indicated that the permutation of subkey bits is performed on the subkey by depending on the value of a j-th data subblock, which is the input data. Therefore, Applicant respectfully requests the Examiner to consider all the limitations in the pending claims.

Furthermore, the newly presented Claim 5 include additional feature of value of another subkey, which is not disclosed or suggested in prior art, including Schneier. The support for can be found in Fig. 1 and page 4, line 13 through page 5, line 18 of the specification.

As previous stated, after studied the Schneier in detail, the Applicant respectfully submits that Fig.12.1 of Schneier shows a general diagram of data conversion in accordance with the encryption algorithm DES (US Data Encryption Standard), which includes 16 rounds of conversion. In each round of conversion, based on a right subblock R and subkey K, function $f = f(R, K)$ is calculated, after which a left subblock L is converted by performing on it the operation XOR: $L := L \oplus f(R, K)$, where ": =" is the designation of assignment operation. Between the preceding and subsequent encryption rounds, the subblocks are permutated. Thus, it is important to ascertain, how conversion $f(R, K)$ is performed. In the Examiner's view, in calculating $f(R, K)$, the operation of permuting subkey bits **depending on data subblock** is used. However, Applicant's detailed study of Schneier has shown that this is not the case. More specifically, Schneier shows that the procedures of calculating the function $f(R, K)$ includes consecutive performing the following operations:

- operation of broadening L 32-bit data subblock to X broadened 48-bit data subblock;
- conversion of the broadened subblock by means of its addition with 48-bit subkey $X := X \oplus K$ (before this step, no conversions depending on the data block being converted have been performed on this round subkey, i.e. **no permuting subkey bits depending on data has been performed);**
- performing a cascade of substitution operations of 6x4 size implementing the substitution operation $\mathbf{S_{6x4}}$, as a result of which the broadened 48-bit subblock is converted into 32-bit binary vector $Z : Z = \mathbf{S_{6x4}}\ (X)$;
- performing the transmutation operation $\boldsymbol{P}$ which consists in a fixed transmutation vector $\boldsymbol{Z}$ bits, i.e. transmutation vector $\boldsymbol{Z}$ bits independently of the value of some data subblock but always in the same manner, as prescribed by Table 12.7 at page 277 of the Schneier reference. After performing operation $\boldsymbol{P}$, the value of $f(R, K)$ is obtained, i.e. we have $f(R, K) = \boldsymbol{P(Z)}$.

The above detailed operations have revealed that, in forming the value of $f(R, K)$ in the DES algorithm, **the operation of permuting subkey bits depending on data being converted is not used**. The vector $\boldsymbol{Z}$ bit transmuting operation performed in the cited method of block encryption (algorithm DES) is fixed and is performed **regardless of data being converted**. Schneier confirms this by describing the operation $\boldsymbol{P}$ in the section "The P-box permutation" (see page 275 and Table 12.7 of Schneier).

The Applicant has also studied the procedures of working-out round subkeys K_1, K_2, ..., K_{16}. According to Schneier, round keys K_1, K_2, ..., K_{16} are generated by means of converting a secret key, on which an operation of fixed transmuting key bits is performed, which depends on the round number but **does not depend on input data**. For a given round, this operation of transmuting key bits is the same for all different datablocks being converted. Following the above fixed key bit transmutation, a fixed compressing key bits transmutation is performed, a result of which is this value of the current round subkey. Fixed compressing key bits transmutation **does not depend on the data begin converted** and remain always the same. Thus, the procedures of forming

round keys of DES algorithm also lacks the feature of "prior to carrying out said two-place operation on an i-th subblock and a subkey, an operation of permuting subkey bits is performed on the subkey **depending on the value of a j-th data subblock**, where $i \neq j$."

Therefore, the newly presented claim is not anticipated by Schneier and the rejection under 35 U.S.C. § 102 (b) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (b) is respectfully requested.

Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: April 12, 2006
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0

By _____
John C. Holman
Registration No. 22,769